AMENDMENTS

In the Claims

Claims 1—71 were pending at the time of the Action.

Claims 1—71 are rejected.

No claims are canceled or amended by the current Response.

New claim 72 was added.

Accordingly, claims 1—72 remain pending and are provided herein below in a complete listing of claims for the sake of convenience:

Listing of Claims:

1. (Original) A method comprising:

verifying that a first application is authorized to set an initial range for a controlled parameter setting;

if authorized, allowing the first application to set an initial range for the controlled parameter setting; and

subsequently, allowing at least a second application to modify the controlled parameter setting within the initial range set by the first application.

2. (Original) A method as recited in claim 1, wherein the first application is verified based on a first security code.

3. (Original) A method as recited in claim 2, wherein the first security code is at least partially encrypted.

4. (Original) A method as recited in claim 1, wherein the first application is verified based at least partially on memory location information associated with a verifying function.

5. (Original) A method as recited in claim 4, wherein the memory location information associated with the verifying function defines memory location within a read only memory (ROM).

6. (Original) A method as recited in claim 1, wherein the initial range includes at least a maximum controlled parameter setting, and the second application is not allowed to modify the controlled parameter setting beyond the maximum controlled parameter setting.

7. (Original) A method as recited in claim 1, wherein the initial range includes at least a minimum controlled parameter setting, and the second application is not allowed to modify the controlled parameter setting below the minimum controlled parameter setting.

8. (Original) A method as recited in claim 1, further comprising:

verifying that the second application is authorized to modify a current range for the controlled parameter setting;

if authorized, allowing the second application to modify the current range for the controlled parameter setting; and

subsequently, allowing at least a third application to modify the controlled parameter setting within the current range as modified by the second application.

9. (Original) A method as recited in claim 8, wherein the second application is verified based on a second security code.

10. (Original) A method as recited in claim 9, wherein the second security code is at least partially encrypted.

11. (Original) A method as recited in claim 8, wherein the second application is verified based at least partially on memory location information associated with a verifying function.

12. (Original) A method as recited in claim 11, wherein the memory location information associated with the verifying function defines memory location within a read only memory (ROM).

13. (Original) A method as recited in claim 8, wherein the current range includes at least a maximum controlled parameter setting, and the third application is not allowed to modify the controlled parameter setting beyond the maximum controlled parameter setting.

14. (Original) A method as recited in claim 8, wherein the current range includes at least a minimum controlled parameter setting, and the third application is not allowed to modify the controlled parameter setting below the minimum controlled parameter setting.

15. (Original) A method as recited in claim 1, wherein the controlled parameter setting is selected from a group of settings comprising an audio volume control parameter, an audio tone control parameter, an illumination control parameter, a visual display control parameter, a temperature control parameter, a communication access control parameter, a peripheral device control parameter, a vehicle control parameter, and an environment control parameter.

16. (Original) A method as recited in claim 8, wherein:

verifying that the first application is authorized to set the initial range for the controlled parameter setting further includes using a first verifier; and

verifying that the second application is authorized to modify the current range for the controlled parameter setting further includes using a second verifier,

wherein the first verifier and the second verifier are operatively configured in a serial arrangement, and the first verifier is independently responsive to a first security code and the second verifier is independently responsive to a second security code.

17. (Original) A method as recited in claim 16, wherein the first verifier is provided by a first entity and the second verifier that is provided by a second entity.

18. (Original) A method as recited in claim 16, wherein the first security code and the second security code are the same.

19. (Original) A method as recited in claim 16, wherein the first security code is provided by a first entity and the second security code is provided by a second entity.

20. (Original) A method as recited in claim 1, wherein verifying that the first application is authorized to set the initial range for the controlled parameter setting further includes using at least one verifier selected from a group comprising at least a first verifier and a second verifier.

21. (Previously presented) A method as recited in claim 8, wherein verifying that the second application is authorized to set the initial range for the controlled parameter setting further includes using at least one verifier selected from a group comprising at least a first verifier and a second verifier.

22. (Original) A computer-readable medium having computer-executable instructions for performing steps comprising:

verifying that a first application is authorized to set an initial range for a controlled parameter setting;

if authorized, allowing the first application to set an initial range for the controlled parameter setting; and subsequently, allowing at least a second application to modify the controlled parameter setting within the initial range set by the first application.

23. (Original) A computer-readable medium as recited in claim 22, wherein the first application is verified based on a first security code.

24. (Original) A computer-readable medium as recited in claim 23, wherein the first security code is at least partially encrypted.

25. (Original) A computer-readable medium as recited in claim 22, wherein the first application is verified based at least partially on memory location information associated with a verifying function.

26. (Original) A computer-readable medium as recited in claim 25, wherein the memory location information associated with the verifying function defines memory location within a read only memory (ROM).

27. (Original) A computer-readable medium as recited in claim 22, wherein the initial range includes at least a maximum controlled parameter setting, and the second application is not allowed to modify the controlled parameter setting beyond the maximum controlled parameter setting.

28. (Original) A computer-readable medium as recited in claim 22, wherein the initial range includes at least a minimum controlled parameter setting, and the second application is not allowed to modify the controlled parameter setting below the minimum controlled parameter setting.

29. (Original) A computer-readable medium as recited in claim 22, having computer-executable instructions for performing steps further comprising:

verifying that the second application is authorized to modify a current range for the controlled parameter setting;

if authorized, allowing the second application to modify the current range for the controlled parameter setting; and

subsequently, allowing at least a third application to modify the controlled parameter setting within the current range as modified by the second application.

30. (Original) A computer-readable medium as recited in claim 29, wherein the second application is verified based on a second security code.

31. (Original) A computer-readable medium as recited in claim 30, wherein the second security code is at least partially encrypted.

32. (Original) A computer-readable medium as recited in claim 29, wherein the second application is verified based at least partially on memory location information associated with a verifying function.

33. (Original) A computer-readable medium as recited in claim 32, wherein the memory location information associated with the verifying function defines memory location within a read only memory (ROM).

34. (Original) A computer-readable medium as recited in claim 29, wherein the current range includes at least a maximum controlled parameter setting, and the third application is not allowed to modify the controlled parameter setting beyond the maximum controlled parameter setting.

35. (Original) A computer-readable medium as recited in claim 29, wherein the current range includes at least a minimum controlled parameter setting, and the third application is not allowed to modify the controlled parameter setting below the minimum controlled parameter setting.

36. (Original) A computer-readable medium as recited in claim 22, wherein the controlled parameter setting is selected from a group of settings comprising an audio volume control parameter, an audio tone control parameter, an illumination control parameter, a visual display control parameter, a temperature control parameter, a communication access control parameter, a peripheral device control parameter, a vehicle control parameter, and an environment control parameter.

37. (Original) A computer-readable medium as recited in claim 29, wherein:

verifying that the first application is authorized to set the initial range for the controlled parameter setting further includes using a first verifier; and

verifying that the second application is authorized to modify the current range for the controlled parameter setting further includes using a second verifier, wherein the first verifier and the second verifier are operatively configured in a serial arrangement, and the first verifier is independently responsive to a first security code and the second verifier is independently responsive to a second security code.

38. (Original) A computer-readable medium as recited in claim 37, wherein the first verifier is provided by a first entity and the second verifier that is provided by a second entity.

39. (Original) A computer-readable medium as recited in claim 37, wherein the first security code and the second security code are the same.

40. (Original) A computer-readable medium as recited in claim 37, wherein the first security code is provided by a first entity and the second security code is provided by a second entity.

41. (Original) A computer-readable medium as recited in claim 22, wherein verifying that the first application is authorized to set the initial range for the controlled parameter setting further includes using at least one verifier selected from a group comprising at least a first verifier and a second verifier.

42. (Original) A computer-readable medium as recited in claim 29, wherein verifying that the first application is authorized to set the initial range for the controlled parameter setting further includes using at least one verifier selected from a group comprising at least a first verifier and a second verifier.

43. (Original) A method comprising:

setting an authorized range and a current value for a controlled parameter;

receiving a request to change the current value of the controlled parameter from an application;

changing the current value of the controlled parameter if a requested value of the controlled parameter is within the authorized range;

otherwise, verifying that the application is authorized to modify the authorized range for the controlled parameter, prior to changing the current value of the controlled parameter to the requested value.

44. (Original) A method as recited in claim 43, wherein verifying that the application is authorized to modify the authorized range for the controlled parameter further comprises changing the authorized range to include the requested value when the application is authorized to modify the authorized range.

45. (Original) A method as recited in claim 44, wherein the authorized range includes at least one authorized limit selected from a group including a minimum authorized limit and a maximum authorized limit.

46. (Original) A method as recited in claim 45, further comprising changing the current value of the controlled parameter to the minimum authorized limit if the requested value is less than the minimum authorized limit and the application is not authorized to modify the authorized range.

47. (Original) A method as recited in claim 45, further comprising changing the current value of the controlled parameter to the maximum authorized limit if the requested value is more than the maximum authorized limit and the application is not authorized to modify the authorized range.

48. (Original) A computer-readable medium having computer-executable instructions for performing steps comprising:

setting an authorized range and a current value for a controlled parameter;

receiving a request to change the current value of the controlled parameter from an application;

changing the current value of the controlled parameter if a requested value of the controlled parameter is within the authorized range;

otherwise, verifying that the application is authorized to modify the authorized range for the controlled parameter, prior to changing the current value of the controlled parameter to the requested value.

49. (Original) A computer-readable medium as recited in claim 48, wherein verifying that the application is authorized to modify the authorized range for the controlled parameter further comprises changing the authorized range to include the requested value when the application is authorized to modify the authorized range.

50. (Original) A computer-readable medium as recited in claim 49, wherein the authorized range includes at least one authorized limit selected from a group including a minimum authorized limit and a maximum authorized limit.

51. (Original) A computer-readable medium as recited in claim 50, further comprising computer-executable instructions for performing the step of changing the current value of the controlled parameter to the minimum authorized limit if the requested value is less than the minimum authorized limit and the application is not authorized to modify the authorized range.

52. (Original) A computer-readable medium as recited in claim 50, further comprising computer-executable instructions for performing the step of changing the current value of the controlled parameter to the maximum authorized limit if the requested value is more than the maximum authorized limit and the application is not authorized to modify the authorized range.

53. (Original) A system comprising:

at least one processor operatively configured to respond to computer instructions associated with a plurality of applications, including a first application;

memory coupled to the processor and configured to store data associated with at least the first application, and

a program operatively configured within the processor and memory and arranged to set a parameter value and a range associated with at least one controlled parameter, determine if the first application is authorized to modify the range, modify the parameter value within the range when requested by the first application, and modify the parameter value outside the range and modify the range when requested by the first application if the first application is authorized to modify the range.

54. (Original) A system as recited in claim 53, wherein the program determines if the first application is authorized to modify the range by analyzing a security code provided by the first application.

55. (Original) A system as recited in claim 54, wherein the program decodes the security code and compares the resulting data to predetermined data to determine if the first application is authorized to modify the range.

56. (Original) A system as recited in claim 54, wherein the program determines that the first application is authorized to change the range only if the security code matches a valid security code.

57. (Original) A system as recited in claim 54, wherein the program further includes at least one linked verifier function stored within a predefined portion of the memory, and the program is configured to determine if the linked verifier function, as called by the program, is not within the predefined portion of the memory, in which case, the program determines that the first application is unauthorized to modify the range.

58. (Original) A system as recited in claim 57, wherein the predefined memory location is within a read only portion of the memory.

59. (Original) A system as recited in claim 54, wherein the security code is uniquely associated a software developer entity responsible for providing the first application.

60. (Original) A system as recited in claim 53, wherein the processor is operatively configured to respond to computer instructions associated with at least a second application, and the program is further configured to determine if the second application is authorized to modify the range, modify the parameter value within the range when requested by the second application, and modify the parameter value outside the range and modify the range when requested by the first application if the first application is authorized to modify the range.

61. (Original) A system as recited in claim 53 wherein the parameter is selected from a group comprising an audio volume control parameter, an audio tone control parameter, an illumination control parameter, a visual display control parameter, a temperature control parameter, a communication access control parameter, a peripheral device control parameter, a vehicle control parameter, and an environment control parameter.

62. (Original) A system as recited in claim 53, wherein the processor, the memory, and the program are part of a computer system within a vehicle.

63. (Original) A system as recited in claim 53, further comprising at least one device that is coupled to the program and is responsive to the parameter value from the program.

64. (Original) An arrangement for use in a computer system, the arrangement comprising:

a parameter manager configurable to receive a parameter change request from one or more computer applications and selectively output a corresponding parameter value;

at least one verifier function accessible by the parameter manager and configured to determine if the parameter change request is from a computer application that is authorized to exceed a parameter limitation; and

a device driver coupled to the parameter manager and configured to receive the parameter value from the parameter manager and output a corresponding control parameter suitable for use by at least one device.

65. (Original) An arrangement as recited in claim 64, wherein the verifier determines if the parameter change request is from the computer application authorized to exceed the parameter limitation by analyzing a security code identified by the first application.

66. (Original) An arrangement as recited in claim 65, wherein the verifier decodes the security code and compares the resulting data to a valid security code to determine if the computer application is authorized to exceed the parameter limitation.

67. (Original) An arrangement as recited in claim 65, wherein at least a portion of the verifier is invoked by the parameter manager in a predefined, identifiable manner, such that if invoked otherwise the computer application is deemed unauthorized to exceed the parameter limitation.

68. (Original) An arrangement as recited in claim 67, further comprising a memory, and wherein the at least a portion of the verifier that is invoked by the parameter manager in a predefined, identifiable manner is associated with at least one memory location within a read only portion of the memory.

69. (Original) An arrangement system as recited in claim 64, wherein the security code is uniquely associated a software developer entity responsible for providing the computer application and the verifier.

70. (Original) An arrangement as recited in claim 64, wherein the parameter manager, verifier, and device driver are part of a computer system within a vehicle.

71. (Original) An arrangement as recited in claim 64, wherein the at least one device includes a computer implemented function.

72. (New) An arrangement as recited in claim 64, wherein the parameter manager is configured to change the corresponding parameter value to a minimum authorized limit if the parameter change request is less than the minimum authorized limit and the verifier function determines the computer application is not authorized to modify the parameter limitation.